The embodiments of the invention in which an exclusive property or privilege is claimed are defined as follows:

1. A method for providing security in a computer system, comprising:

selecting a set of properties for use in determining members of a clean group; and

evaluating an item to determine if it has the specified set of properties, and if the item does have the specified set of properties, designating it as a member of the clean group.

2. The method of Claim 1, wherein the items are computers.

3. The method of Claim 2, wherein when a computer is to be evaluated, a clean component is installed on the computer to perform compliance checks.

4. The method of Claim 1, wherein a compliance check is performed at a selected time for an item to determine if the item has the specified set of properties.

5. The method of Claim 1, wherein one of the specified set of properties is whether all of the available updates have been installed.

6. The method of Claim 5, wherein the updates comprise at least one of security updates or service packs.

7. The method of Claim 4, wherein if the compliance check fails, a message is sent to indicate that the object should not be in the clean group.

8. The method of Claim 7, wherein if the compliance check fails, the clean group membership of the item is invalidated.

9. The method of Claim 8, wherein the invalidation of the clean group membership comprises local actions which may include at least one of hiding or erasing the domain credentials of the item.

10. The method of Claim 7, wherein if the compliance check fails, additional steps may be taken including at least one of hiding cryptographic keys or logging out a privileged user.

11. The method of Claim 4, wherein if a compliance check passes, a message is sent to provide information that will be evaluated to determine if the item should be in the clean group.

12. The method of Claim 11, wherein after a message is received and a determination is made that the item should be in the clean group, a countdown is started and if another message is not received by the end of the countdown, the item is removed from the clean group.

13. The method of Claim 1, wherein an item in the clean group performs a self check to determine if it still has the specified set of properties, and if it does not, takes action to have itself removed from the clean group.

14. The method of Claim 1, further comprising a clean group server, the clean group server initiating a status check to determine if the members in the clean group still have the specified properties.

15. A system for managing security, comprising:

an update component which includes updates for items;

a clean runtime component, the clean runtime component being installed on an item and being able to communicate with the update component, the item becoming a member of a clean group when selected criteria are met; and

a clean group server.

16. The system of Claim 15, further comprising a domain controller which communicates with the clean group server.

17. The system of Claim 15, wherein the items comprise computers.

18. The system of Claim 17, wherein compliance checks are performed for the items to determine if the items meet the selected criteria.

19. The system of Claim 18, wherein one of the criteria is whether selected available updates have been installed.

20. The system of Claim 19, wherein the updates comprise at least one of security updates or service packs.

21. The system of Claim 18, wherein if a compliance check fails, a message is sent from the clean runtime component to the clean group server to indicate that the item should not be in the clean group.

22. The system of Claim 18, wherein if the compliance check passes, a message is sent from the clean runtime component to the clean group server to provide information that will be used to evaluate whether the item should be in the clean group.

23. The system of Claim 22, wherein after a message is received to indicate that the item should be placed in the clean group, a countdown is started and if another message is not received by the end of the countdown, the item is removed from the clean group.

24. The system of Claim 15, wherein the clean runtime component performs a self-check of the item to determine if it meets the selected criteria for remaining in the clean group.

25. The system of Claim 15, wherein the clean group server initiates a compliance check for items to determine if they should remain in the clean group.

26. One or more computer-readable media for providing security in a computer system, comprising:

a runtime object which is installed on a computer, the runtime object being run on the computer to determine if the computer is in compliance, and based on the results of the compliance check sends a message regarding whether the computer should be in a group.

27. The media of Claim 26, wherein the compliance check is performed initially upon installation of the runtime object.

28. The media of Claim 26, wherein the compliance check comprises a determination of whether selected available updates have been installed on the computer.

29. The media of Claim 28, wherein the selected available updates comprise at least one of security updates or service packs.

30. The media of Claim 26, wherein after a message is received to indicate that the computer should be placed in the group, a countdown is started and if another message is not received by the end of the countdown, the item is removed from the group.

31. The media of Claim 26, wherein the clean runtime object performs a compliance check on the computer.

32. The media of Claim 26, wherein a group server communicates with the runtime object to initiate a compliance check.

33. A method for providing security in a computer system, comprising:

determining if a computer is in compliance; and

based on whether or not the computer is in compliance, disabling or enabling the computer domain account.

34. The method of Claim 33, wherein when a new computer is to be added to the domain account, the new computer's account is placed in a disabled state until the computer is proved to be in compliance.

35. The method of Claim 33, wherein when a new computer is to be added to the domain account, the domain join operation is predicated on proving that the computer is in compliance by requiring a clean group server to participate in the domain join operations.

36. The method of Claim 33, wherein the compliance check comprises determining whether available updates have been installed on the computer.

37. The method of Claim 33, wherein the computer periodically performs compliance checks.

38. The method of Claim 33, wherein a clean group server periodically initiates a compliance check on the computer.

39. A method for providing security in a computer system, comprising:
performing compliance checks for items;
placing items which pass the compliance check into a clean group; and
removing items from the clean group which fail the compliance check.

40. The method of Claim 39, wherein after an item passes a compliance check and is placed in the clean group, a countdown is started and if another compliance check is not passed by the end of the countdown, the item is removed from the clean group.

41. The method of Claim 39, wherein the item is a computer.

42. The method of Claim 39, wherein the item performs a compliance check.

43. The method of Claim 39, wherein a clean group server initiates a compliance check on the item.

44. The method of Claim 39, wherein the compliance check is performed by the item communicating with an update Web site to determine if updates are available for the item.

45. The method of Claim 44, wherein the item communicates with a clean group server to establish its membership in the clean group.

46. The method of Claim 45, wherein the clean group server communicates with a domain controller.

47. The method of Claim 39, wherein a compliance check may be initiated by one or more of a client coming online, changes in client status/configuration, changes in network status/configuration, or changes to a compliance policy.

48. The method of Claim 39, wherein a clean group server communicates to non-compliant items how to get back into compliance.

49. The method of Claim 48, wherein the non-compliant items are directed to a Web site with online instructions to the user, and once the instructions are followed, another server-assisted compliance check is initiated.

50. The method of Claim 48, wherein the non-compliant items are instructed how to get into the compliant state automatically without requiring a user's involvement.

51. The method of Claim 39, wherein an item may be a user, and a user's clean group membership is evaluated on the basis of whether the user's computer is in compliance.

52. The method of Claim 39, wherein a clean group is utilized to implement a computer security policy.

53. The method of Claim 52, wherein the clean group is utilized to provide enforcement of the computer security policy by binding active directory group policy to the group membership such that only members of the group can read the policy.

54. The method of Claim 53, wherein the policy provides IPSec communication requirements and parameters.

55. The method of Claim 54, wherein only computers which comply with the policy and are thus members of the clean group can read the IPSec policy parameters and thus communicate with one another, while computers which are not members of the clean group are effectively prevented from communicating with computers in the clean group, thus in effect providing a quarantine mechanism.

56. The method of Claim 55, wherein a client that changes state from membership in the clean group to non-membership is required to clear all policy settings distributed via the clean group.

57. A method for providing security in a computer system, comprising:

performing a compliance check for an item; and

based on the results of the compliance check determining whether the item should be in a group.

58. The method of Claim 57, wherein if the item passes the compliance check, it is placed in a clean group.

59. The method of Claim 57, wherein if the item fails the compliance check, it is placed in a dirty group.